CLAIMS

1. A method of establishing a secure communication link between a smart card and a central computer system through a communication network, the method comprising the steps of:

demodulating an outgoing secure radio frequency signal transmitted from the smart card to produce an outgoing secure data signal;

formatting the outgoing secure data signal in accordance with a communication network protocol to produce an outgoing formatted secure signal; and

transmitting the outgoing formatted secure signal to the central computer system.

2. A method in accordance with claim 1 further comprising the step of subjecting outgoing secure data contained within the outgoing secure radio frequency signal to a security function only at the smart card and at the central computer system.

3. A method in accordance with claim 1, wherein the step of demodulating the outgoing secure radio frequency signal comprises the step of demodulating the outgoing secure radio frequency signal without deciphering the outgoing secure data signal.

4. A method in accordance with claim 1 further comprising the steps of:

reformatting, at the central computer system, the outgoing formatted secure signal to produce the outgoing secure data signal; and

decoding, at the central computer system, the outgoing secure data signal to receive smart card information included within the outgoing secure data signal.

5. A method in accordance with claim 4 further comprising the steps of:

receiving an incoming secure formatted signal from the central computer system through the communication network, the incoming secure formatted signal formatted in accordance with the communication network protocol;

reformatting the incoming secure formatted signal to produce an incoming secure data signal; and

transmitting an incoming secure radio frequency signal to the smart card, wherein the incoming secure radio frequency signal is modulated in accordance with the incoming secure data signal.

6. A method in accordance with claim 5 further comprising the steps of:

demodulating the incoming secure radio frequency signal within the smart card to produce the incoming secure data signal; and

decoding the incoming secure data signal to receive central computer information included within the incoming secure data signal.

7. A method in accordance with claim 6 wherein the step of decoding the outgoing secure data signal comprises the step of implementing a security function using a security device coupled to the central computer system to decode the outgoing secure data signal.

8. A method in accordance with claim 7 further comprising the step of encoding outgoing data within the smart card using a security function to produce the outgoing secure data signal.

9. A method in accordance with claim 8 wherein the step of encoding further comprises the steps of :

generating a message authentication code at the smart card; and

appending the message authentication code to the outgoing data.

10. A method in accordance with claim 9, wherein the step of decoding comprises the step of observing a characteristic of the outgoing data in accordance with the message authentication code.

11. A method in accordance with claim 10, wherein the step of observing comprises the step of:

generating the message authentication code at the central computer system; and

comparing the secure outgoing data signal to the message authentication code to detect an unauthorized modification of the outgoing data.

12. A method in accordance with claim 10 wherein the step of decoding the incoming secure data signal comprises the step of decoding the incoming secure data signal within the smart card using a security function.

13. A method in accordance with claim 7 further comprising the step of encoding incoming data within the central computer system using a security function to produce the incoming secure data signal.

14. A method in accordance with claim 13 wherein the step of encoding further comprises the steps of :

generating a message authentication code at the central computer system; and

appending the message authentication code to the incoming data.

15. A method in accordance with claim 14, wherein the step of decoding comprises the step of observing a characteristic of the incoming in accordance with the message authentication code.

16. A method in accordance with claim 15, wherein the step of observing comprises the step of:

generating the message authentication code at the smart card; and

comparing the secure incoming data signal to the message authentication code to detect an unauthorized modification of the incoming data.

17. A method of establishing a secure communication link between a smart card and a central computer system through a communication network, the method comprising the steps of:

encoding smart card information within the smart card using a security function to produce an outgoing secure data signal;

transmitting an outgoing secure radio frequency signal including the outgoing secure data signal to a smart card communication device;

demodulating an outgoing secure radio frequency signal at the smart card communication device to produce the outgoing secure data signal;

formatting the outgoing secure data signal in accordance with a communication network protocol to produce an outgoing formatted secure signal;

transmitting the outgoing formatted secure signal to the central computer system through a communication network;

reformatting the outgoing formatted secure signal to produce the outgoing secure data signal; and

decoding, using a security device coupled to the central computer system, the outgoing secure data signal to receive the smart card information;

encoding central computer system information using the security device to produce an incoming secure data signal;

formatting the incoming secure data signal to produce an incoming secure formatted signal;

receiving the incoming secure formatted signal from the central computer system through the communication network, the incoming secure formatted signal formatted in accordance with the communication network protocol;

reformatting the incoming secure formatted signal to produce the incoming secure data signal; and

transmitting an incoming secure radio frequency signal to the smart card, wherein the incoming secure radio frequency signal is modulated in accordance with the incoming secure data signal;

demodulating the incoming secure radio frequency signal within the smart card to produce the incoming secure data signal; and

decoding the incoming secure data signal using a security function to receive the central computer information at the smart card.

18. A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

exchanging secure data through a radio frequency communication channel with the smart card;

exchanging the secure data through a communication network with the central computer system; and

performing a security function on the data at the central computer system.

19. A method in accordance with claim 18, further comprising the step of performing a security function on the at the smart card.

20. A method in accordance with claim 18 wherein the step of exchanging the secure data through the communication network comprises the steps of:

formatting secure data in accordance with a communication network protocol;

transmitting the secure data through the communication network;

and reformatting the secure data.

21. A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

downloading communication link interface software to a processor from a remote computer system;

exchanging secure data between the smart card and a smart card communication device through a radio frequency communication channel; and

exchanging the secure data between the smart card communication device and the central computer system through the processor running the downloaded communication link interface software, wherein the processor is coupled to the central computer system through a communication network.

22. A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

exchanging secure data with a smart card communication device through a baseband data channel, wherein the secure data corresponds to secure data exchanged between the smart card communication device and the smart card through a radio frequency channel,

formatting the secure data in accordance with a communication network protocol; and

exchanging the secure data with the central computer system through a communication network.

23. A method in accordance with claim 22 wherein the secure data is not deciphered within the communication link.

24. A method in accordance with claim 22 further comprising the step of subjecting the secure data to a security function only at the smart card and at the central computer system.

25. A smart card communication system for establishing a secure communication link between a smart card and a central computer system, the smart card communication system comprising:

a smart card communication device comprising a radio frequency transceiver adapted to exchange secure data with the smart card through a radio frequency communication channel and a data communication interface;

a processor coupled to the smart card communication device, the processor adapted to exchange the secure data with the data communication interface through a baseband data channel;

a communication network coupled to the processor and adapted to exchange the secure data in accordance with a communication network protocol between the processor and the central computer system; and

a security device coupled to the central computer system.

26. A system in accordance with claim 25 wherein the communication network is an Internet network and the communication network protocol is an Internet protocol.

27. A system in accordance with claim 25 further comprising a smart card adapted to subject outgoing data to a security function to produce a secure outgoing data signal.

28. A system in accordance with claim 25 further comprising a smart card adapted to subject a secure incoming data signal to a security function to produce deciphered incoming data.

29. A smart card communication device for interfacing within a smart card communication system having a local processor coupled to a remotely located central computer system through a communication network, the smart card communication device comprising:

a radio frequency transceiver adapted to exchange secure data with a smart card through a radio frequency communication channel;

a data communication interface adapted to exchange the secure data with the processor through a baseband data communication channel without deciphering the secure data.

30. A device in accordance with claim 29 wherein the transceiver comprises:

a receiver adapted to receiving a secure outgoing radio frequency signal from a smart card to produce a secure outgoing data signal, the data communication interface adapted to send the outgoing data signal through the baseband data channel in a secure state.

31. A device in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to produce the secure outgoing data signal, the secure outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to an intelligible message only when subjected to a security function.

32. A device in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to produce the secure outgoing data signal, the secure

outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

33. A device in accordance with claim 29 wherein the transceiver comprises a transmitter adapted to transmit a secure incoming radio frequency signal to the smart card, the secure incoming radio frequency signal based on a secure incoming data signal received by the data communication interface.

34. A device in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality of logic highs and plurality of logic lows corresponding to an intelligible message when subjected to a security function.

35. A device in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality of logic highs and plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

36. A method of providing access to data stored on a smart card, the method comprising the steps of:

providing a transaction form Web page at a local processor; and

performing a transaction in accordance with information submitted by the customer in the transaction form Web page.

37. A method in accordance with claim 36 wherein the step of providing is performed by a remote central computer system coupled to the local processor through a network.

38. A method in accordance with claim 37 wherein the step of performing the transaction is performed by the remote central computer system.

39. A method in accordance with claim 38 wherein the information submitted by the customer in the transaction form Web page includes credit card information.

40. A method in accordance with claim 39 wherein the credit card information submitted by the customer in the transaction form Web page is verified for availability of funds by the central computer system.

41. A method of establishing a communication link between a smart card and a central computer system, the method comprising the steps of:

applying an authentication function to data at the smart card and the central computer system; and

exchanging the data through a communication network between the smart card and the central computer system.

42. A method in accordance with claim 41 further comprising the step of detecting an unauthorized modification to the data.

43. A method in accordance with claim 42 wherein the unauthorized modification to the data is an intentional fraudulent modification.

44. A method in accordance with claim 40 wherein the unauthorized modification to the data is due to an error in transmission through the communication network.

45. A method in accordance with claim 41, wherein the step of applying the authentication function comprises the steps of:

transmitting the data from the smart card with a message authentication code generated at the smart card;

generating the message authentication code at the central computer system; and

verifying the data at the central computer system using the message authentication code.

46. A method in accordance with claim 41, wherein the step of applying the authentication function comprises the steps of:

transmitting the data from the central computer system with a message authentication code generated at the central computer system; and

generating the message authentication code at the smart card; and

verifying the data at the smart card using the message authentication code.

47. A method in accordance with claim 41, further comprising the step of downloading, at a local processor coupled between the smart card and the communication network, a temporary software application to facilitate the exchange of data through the network.

48. A method in accordance with claim 47, wherein the step of downloading comprises the step of downloading a Java applet.

49. A method of establishing a communication link between a smart card and a central computer through a communication network, the method comprising the step of:

downloading a temporary software application to a local processor coupled between the smart card and the communication network;

executing the temporary software application on the local processor to exchange data between the smart card and the central computer system.

50. A smart card communication system comprising:

a smart card;

a central computer system:

a communication network coupled between the smart card and the central computer system;

a local processor coupled to the smart card and the communication network, the local processor adapted to execute a temporary

software application downloaded through the network to establish a communication link between the smart card and the central computer system

51. A smart card communication system in accordance with claim 50, wherein the temporary software application is a Java applet.

52. A smart card communication system in accordance with claim 50 further comprising a smart card communication device coupled to the smart card through a first channel and coupled to the local processor through a second channel, the smart card communication device exchanging data between the smart card and the local processor.

53. A system in accordance with claim 52, wherein the first channel is a radio frequency channel; and wherein the second channel is baseband data channel.

54. A smart card communication system comprising:

a communication network coupled between a smart card and the central computer system;

the smart card comprising a first security device adapted to generate a message authentication code to authenticate data exchanged between the smart card and the central computer system;

the central computer system comprising a second security device adapted to generate the message authentication code to authenticate the data, the data maintained in an authenticated state between the smart card and the central computer system.

55. A smart card communication system in accordance with claim 54 wherein the smart card is adapted to authenticate outgoing data by appending a message authentication code generated by the first security device to the outgoing data.

56. A smart card communication system in accordance with claim 55 wherein the central computer system is adapted to authenticate the outgoing data by detecting an absence of an unauthorized modification of the incoming

data based on the message authentication code, the message authentication code generated by the second security device.

57. A smart card communication system in accordance with claim 54 wherein the central computer is adapted to authenticate incoming data for transmission to the smart card by appending a message authentication code generated by the second security device to the incoming data.

58. A smart card communication system in accordance with claim 57 wherein the smart card is adapted to authenticate an incoming data of an incoming data signal transmitted by the central computer system by detecting an absence of an unauthorized modification of the incoming data based on the message authentication code, the message authentication code generated by the first security device.